Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

multiplexer circuitry having an input stage and an output stage;

expansion logic coupled to the input stage of the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence corresponding to a first portion of the data block, wherein the output of the expansion logic is coupled to the input stage of the multiplexer circuitry;

~~first and second registers coupled to the output stage of the multiplexer circuitry, wherein the multiplexer circuitry selects between the first and second registers and stores the output of the expansion logic in a selected register;~~ and

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the first portion of the data block, wherein the second bit sequence is derived from R XOR $P^{-1}(L)$, where R is a third bit sequence based on the expanded first bit sequence, and $P^{-1}(L)$ is an inverse permutation of a bit sequence

corresponding to a second portion of the data block, the inverse permutation being performed by an inverse permutation logic performing reverse operations of the permutation logic. ~~whereby altering the second bit sequence performs cryptographic operations on the data block.~~

2. (Original) The cryptography engine of claim 1, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

3. (Original) The cryptography engine of claim 1, wherein the cryptography engine is a DES engine.

4. (Previously Presented) The cryptography engine of claim 1, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on a first level coupled to two 2-to-1 multiplexers on a second level.

5. (Original) The cryptography engine of claim 1, wherein the first bit sequence is less than 32 bits.

6. (Original) The cryptography engine of claim 1, wherein the first bit sequence is four bits.

7. (Original) The cryptography engine of claim 5, wherein the expanded first bit sequence is less than 48 bits.

8. (Original) The cryptography engine of claim 6, wherein the expanded first bit sequence is less than six bits.

9. (Previously Presented) The cryptography engine of claim 2, wherein the third bit sequence is less than 48 bits.

10. (Previously Presented) The cryptography engine of claim 2, wherein the third bit sequence is six bits.

11. (Original) The cryptography engine of claim 9, wherein the second bit sequence is less than 32 bits.

12. (Original) The cryptography engine of claim 10, wherein the second bit sequence is four bits.

13. (Original) The cryptography engine of claim 1, wherein the multiplexer circuitry is a two-level multiplexer.

14. (Previously Presented) The cryptography engine of claim 13, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

15. (Original) The cryptography engine of claim 1, wherein the expansion logic and the permutation logic are associated with DES operation.

16. (Original) The cryptography engine of claim 1, wherein the key scheduler performs pipelined key scheduling logic.

17. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a determination stage.

18. (Original) The cryptography engine of claim 1, wherein the key schedule comprises a shift stage.

19. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a propagation stage.

20. (Original) The cryptography engine of claim 1, wherein the key scheduler comprises a consumption stage.

21. (Previously Presented) The cryptography engine of claim 17, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

22. (Currently Amended) A cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising:

a key scheduler configured to provide keys for cryptographic operations;

multiplexer circuitry having an input stage and an output stage;

expansion logic coupled to the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block;

~~first and second registers coupled to the output stage of the multiplexer circuitry, wherein the multiplexer circuitry selects between the first and second registers and stores the output of the expansion logic in a selected register;~~

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block; and

inverse permutation logic coupled to the input stage of the multiplexer circuitry, the inverse permutation logic performing reverse operations of the permutation logic.

23. (Original) The cryptography engine of claim 22, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

24. (Original) The cryptography engine of claim 22, wherein the cryptography engine is a DES engine.

25. (Previously Presented) The cryptography engine of claim 22, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on a first level coupled to two 2-to-1 multiplexers on a second level.

26. (Original) The cryptography engine of claim 22, wherein the first bit sequence is less than 32 bits.

27. (Original) The cryptography engine of claim 22, wherein the first bit sequence is four bits.

28. (Original) The cryptography engine of claim 26, wherein the expanded first bit sequence is less than 48 bits.

29. (Original) The cryptography engine of claim 27, wherein the expanded first bit sequence is less than six bits.

30. (Previously Presented) The cryptography engine of claim 23, wherein the third bit sequence is less than 48 bits.

31. (Previously Presented) The cryptography engine of claim 23, wherein the third bit sequence is six bits.

32. (Original) The cryptography engine of claim 30, wherein the second bit sequence is less than 32 bits.

33. (Original) The cryptography engine of claim 31, wherein the second bit sequence is four bits.

34. (Original) The cryptography engine of claim 22, wherein the key scheduler performs pipelined key scheduling logic.

35. (Original) The cryptography engine of claim 22, wherein the key scheduler comprises a plurality of stages.

36. (Original) The cryptography engine of claim 22, wherein the key scheduler comprises a determination stage.

37. (Original) The cryptography engine of claim 22, wherein the key scheduler comprises a shift stage.

38. (Original) The cryptography engine of claim 22, wherein the key scheduler comprises a propagation stage.

39. (Original) The cryptography engine of claim 22, wherein the key scheduler comprises a consumption stage.

40. (Previously Presented) The cryptography engine of claim 36, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

41. (Original) The cryptography engine of claim 22, wherein the multiplexer circuitry is a two-level multiplexer.

42. (Previously Presented) The cryptography engine of claim 41, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

43. (Original) The cryptography engine of claim 22, wherein the expansion logic and the permutation logic are associated with DES operations.

44. (Currently Amended) An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine, the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations;

multiplexer circuitry having an input and an output stage;

expansion logic coupled to the input stage of the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a first portion of the data block, wherein the output of the expansion logic is coupled to the input stage of the multiplexer circuitry;

~~first and second registers coupled to the output stage of the multiplexer circuitry, wherein the multiplexer circuitry selects between the first and second registers and stores the output of the expansion logic in a selected register;~~ and

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the first portion of the data block, wherein the second bit sequence is derived from R XOR $P^{-1}(L)$, where R is a third bit sequence based on the expanded first bit sequence, and $P^{-1}(L)$ is an inverse permutation of a bit sequence corresponding to a second portion of the data block, the inverse permutation being performed by an inverse permutation logic performing reverse operations of the permutation logic. ~~whereby altering the second bit sequence performs cryptographic operations on the data block~~.

45. (Previously Presented) The integrated circuit layout of claim 44, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

46. (Previously Presented) The integrated circuit layout of claim 44, wherein the cryptography engine in a DES engine.

47. (Previously Presented) The integrated circuit layout of claim 44, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on a first level coupled to two 2-to-1 multiplexers on a second level.

48. (Previously Presented) The integrated circuit layout of claim 44, wherein the first bit sequence is four bits.

49. (Previously Presented) The integrated circuit layout of claim 48, wherein the expanded first bit sequence is less than six bits.

50. (Previously Presented) The integrated circuit layout of claim 44, wherein the key scheduler performs pipelined key scheduling logic.

51. (Previously Presented) The integrated circuit layout of claim 44, wherein the key scheduler comprises a determination stage, a shift stage, a propagation stage, and a consumption stage.

52. (Previously Presented) The integrated circuit layout of claim 51, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

53. (Previously Presented) The integrated circuit layout of claim 44, wherein the multiplexer circuitry is a two-level multiplexer.

54. (Previously Presented) The integrated circuit layout of claim 53, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

55. (Previously Presented) The integrated circuit layout of claim 44, wherein the expansion logic and the permutation logic are associated with DES operations.

56. (Currently Amended) An integrated circuit layout associated with a cryptography engine for performing cryptographic operations on a data block, the integrated circuit layout providing information for configuring the cryptography engine, the integrated circuit layout comprising:

a key scheduler configured to provide keys for cryptographic operations;

multiplexer circuitry having an input stage and an output stage;

expansion logic coupled to the multiplexer circuitry, the expansion logic configured to expand a first bit sequence having a first size to an expanded first bit sequence having a second size greater than the first size, the first bit sequence corresponding to a portion of the data block;

~~first and second registers coupled to the output stage of the multiplexer circuitry, wherein the multiplexer circuitry selects between the first and second registers and stores the output of the expansion logic in a selected register;~~

permutation logic coupled to the expansion logic, the permutation logic configured to alter a second bit sequence corresponding to the portion of the data block, whereby altering the second bit sequence performs cryptographic operations on the data block; and

inverse permutation logic coupled to the input stage of the multiplexer circuitry, the inverse permutation logic performing reverse operations of the permutation logic.

57. (Previously Presented) The integrated circuit layout of claim 56, further comprising an Sbox configured to alter a third bit sequence corresponding to the portion of the data block by compacting the size of the third bit sequence and altering the third bit sequence using Sbox logic.

58. (Previously Presented) The integrated circuit layout of claim 56, wherein the cryptography engine is a DES engine.

59. (Previously Presented) The integrated circuit layout of claim 56, wherein the multiplexer circuitry comprises two 2-to-1 multiplexers on a first level coupled to two 2-to-1 multiplexers on a second level.

60. (Previously Presented) The integrated circuit layout of claim 56, wherein the first bit sequence is four bits.

61. (Previously Presented) The integrated circuit layout of claim 60, wherein the expanded first bit sequence is less than six bits.

62. (Previously Presented) The integrated circuit layout of claim 56, wherein the key scheduler performs pipelined key scheduling logic.

63. (Previously Presented) The integrated circuit layout of claim 56, wherein the key scheduler comprises a determination stage, a shift stage, a propagation stage, and a consumption stage.

64. (Previously Presented) The integrated circuit layout of claim 63, wherein a first shift amount for a first key is identified in the determination stage using a first round counter value.

65. (Previously Presented) The integrated circuit layout of claim 56, wherein the multiplexer circuitry is a two-level multiplexer.

66. (Previously Presented) The integrated circuit layout of claim 65, wherein the two-level multiplexer is configured to select either initial data, swapped data, or non-swapped data to provide to the output stage of the multiplexer.

67. (Previously Presented) The integrated circuit layout of claim 56, wherein the expansion logic and the permutation logic are associated with DES operations.